

EX PARTE OR LATE FILED
DOCKET FILE COPY ORIGINAL



Frank S. Simone
District Manager - Federal Government Affairs

Room 1117L2
295 North Maple Avenue
Basking Ridge, NJ 07920
(908) 221 - 7206

July 14, 1994

Mr. William F. Caton, Acting Secretary
Federal Communications Commission
1919 M Street, N.W. -- Room 222
Washington, D. C. 20554

RECEIVED
JUL 14 1994
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF SECRETARY

Re: Ex Parte Presentation - CC Docket No. 93-292, Toll Fraud

Dear Mr. Caton:

A meeting was held today with Linda DuBroof of the Domestic Facilities Division and AT&T, represented by Richard Bleicher, Thomas Munger and myself, to discuss AT&T's position in the proceeding indicated above. The attached material was used during the course of our meeting.

Pursuant to Section 1.1206(a)(1) of the Commission's Rules, an original and two copies of this notice are attached. Please contact me if you have any questions concerning this matter.

Sincerely,

A handwritten signature in cursive script, appearing to read "F S Simone".

ATTACHMENT

Computer L. DuBroof

AGENDA

RECEIVED

JUL 14 1994

**FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF SECRETARY**

**PRESENTATION TO THE
FEDERAL COMMUNICATIONS COMMISSION
JULY 14, 1994**

**By: Richard Bleicher and
Thomas Munger**

**RECENT AT&T GBCS TOLL FRAUD SECURITY
INITIATIVES DEMONSTRATE AT&T'S CONTINUED
LEADERSHIP IN COMMUNICATIONS SYSTEM
SECURITY**

COMMUNICATIONS INITIATIVES

- Certified Mailing
- Expert Computer System "Screener"
- Security Handbook & Individual Learning Program Sent Free to GBCS Service Agreement and Warranty Customers

TECHNOLOGY INITIATIVES

- AT&T Definity® G3V3 PBX
- AT&T INTUITY™ Messaging System

SUPPORT PROCESS INITIATIVES

- Secure System Installation Procedure
- NetPROTECTsm/GBCS Operational Customer Hand off

FRAUD RESOLUTION PROCESS

COMMUNICATIONS INITIATIVES

Certified Toll Fraud Warning Letter (March, 1994)

- Warning letter and instructional booklet sent to approximately 32,000 DEFINITY PBX and Audix voice mail customers.
- Letter sent CERTIFIED, to highlight significance of letter's contents.

(Attachment)

COMMUNICATIONS INITIATIVES

Expert Computer System "Screener" (April-May, 1994)

- AT&T's Expert Computer System (remote maintenance platform) calls the customer's AT&T PBX and performs security screening for:
 - Default customer administration passwords;
 - DISA feature activation;
 - DISA Barrier Code length;
- To date, AT&T has performed this screening at no charge for approximately 30,000 AT&T PBXs.
- AT&T sends personalized letter to customer reviewing findings (whether or not security weaknesses were found).
- Offers AT&T assistance to secure any security weakness.

COMMUNICATIONS INITIATIVES

AT&T GBCS Products Security Handbook (June, 1994)

- Issue 3 produced in March, 1994.
- Provided with the AT&T product at no charge with all AT&T PBX and voice messaging products.
- Mailed with the Individualized Learning Program, at no charge to all GBCS service agreement customers.

(Attachment)

TECHNOLOGY INITIATIVES

DEFINITY® G3V3 Communications Systems (March, 1994)

- Current PBX offer.
- Major investment in market-defined security platform.
- Security Enhancement includes:
 - Secure system administration approach -- customer must create login and password in order to perform system administration;
 - Option to permanently disable DISA;
 - Optional "aging" feature for passwords and Barrier Codes;
- Clear and explicit security warning contained in all product documentation.

TECHNOLOGY INITIATIVES

AT&T INTUITY™ Messaging System (January, 1994)

- Current messaging platform (multi-media: voice, video, e-mail, fax).
- Major investment in market-defined security platform:
 - Secure transfer option cannot be changed without explicit warning;
 - Option for forced aging of mailbox passwords.

SUPPORT PROCESS INITIATIVES

Secure System Installation Procedure (May, 1994)

- Requires security awareness discussion before signing equipment contract.
- Establishes security roles and responsibilities.
- Utilizes a security checklist to insure a secure system.

SUPPORT PROCESS INITIATIVES

AT&T NetPROTECTSM Service/ GBCS Operational Process (July, 1994)

- Operational process goal - to stop fraud upon detection.
- When toll fraud is detected by AT&T NetPROTECT and confirmed by customer, if customer has GBCS equipment, customer call conferenced with GBCS Technical Service Center.

FRAUD RESOLUTION PROCESS

- Provides a formal process whereby customers can file toll fraud claims against AT&T.
- Hundreds of claims settled, less than 2% litigated.
- Each claim investigated and addressed individually.
- Customers overwhelmingly satisfied with this process.

Copyright© 1993 AT&T
All Rights Reserved
Printed in USA

Published by
GBCSystems Product Documentation Development
AT&T Bell Laboratories
Middletown, NJ 07748-1976

Notice

While reasonable effort was made to ensure that the information in this document was complete and accurate at the time of printing, AT&T cannot assume responsibility for any errors. Changes and/or corrections to the information contained in this document may be incorporated into future issues.

Your Responsibility for Your System's Security

Toll fraud, the unauthorized use of your telecommunications system by an unauthorized party (e.g., persons other than your company's employees, agents, subcontractors, or persons working on your company's behalf) can result in substantial additional charges for your telecommunications services. You are responsible for the security of your system. There may be a risk of toll fraud associated with your telecommunications system. You are responsible for programming and configuring your equipment to prevent unauthorized use. Your system administrator should read all installation, instruction, and system administration documents provided with this product to fully understand the features that can introduce the risk of toll fraud and the steps that can be taken to reduce that risk. AT&T does not warrant that this product is immune from or will prevent unauthorized use of common-carrier telecommunication services or facilities accessed through or connected to it. AT&T will not be responsible for any charges that result from such unauthorized use. Updates are available through AT&T ACCESS Electronic News and InfoShare, or THE AT&T CATALOG Fax Attendant.

Federal Communications Commission (FCC) Statement

This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.

Operation of this equipment in a residential area is likely to cause interference, in which case the user at his or her own expense will be required to take whatever measures may be required to correct the interference.

Trademarks

AUDIX, CALLMASTER, CONVERSANT, DEFINITY, MERLIN, MERLIN LEGEND, and PARTNER are registered trademarks of AT&T.
HackerTracker, INTUITY, MERLIN MAIL, PARTNER MAIL, TransTalk, and Voice Power are trademarks of AT&T.
Carbon Copy Plus is a trademark of Microcom Inc.
Netware is a registered trademark of Novell Inc.
Norton pcANYWHERE is a registered trademark of Symantic Corporation.
UNIX is a registered trademark of UNIX System Laboratories, Inc.
NetPROTECT is a service mark of AT&T.

In this document, DEFINITY Communications System Generic 1, 2, or 3 is often abbreviated to DEFINITY G1, G2, or G3.

Ordering Information

Call: AT&T Customer Information Center
1 800 432-6600
In Canada: 1 800 255-1242

Write: AT&T Customer Information Center
2855 North Franklin Road, P.O. Box 19901
Indianapolis, IN 46219-1385

Order: Document No. AT&T 555-025-600
Issue 3, March 1994

Acknowledgment

This document was developed by AT&T in conjunction with input from the Security Committee of the Global and National DEFINITY User Groups. In addition, certain materials contained in this document were extracted from the Step by Step Security Guide, a valuable tool developed by the members of this committee. Grateful thanks are owed to the Security Committee members for their assistance and for their willingness to share this information.